



# Medical Device Security: Where are We Going?



## Kevin Fu, Ph.D.

University of Michigan

Director, Archimedes Center for Medical Device Security

Associate Professor, Electrical Engineering & Computer Science

[secure-medicine.org](mailto:secure-medicine.org)    [kevinfu@umich.edu](mailto:kevinfu@umich.edu)

**Archimedes:**  
Safety-Centric  
Cybersecurity  
Education



FDA Patient Engagement Advisory Committee, September 10, 2019

# Disclosures

- Co-founder, healthcare security startup **VIRTA LABS™**
- Director, Archimedes Center for Medical Device Security
- Fmr. visiting scientist, U.S. Food and Drug Administration
- Consultant to MITRE, Medtronic, and Novartis Pharmaceuticals
- Recent re\$earch \$upport:

- Archimedes supported by institutional members





**ARCHIMEDES**  
MEDICAL DEVICE SECURITY  
RESEARCH CENTER



**I Am The Cavalry**

**Thank You.**



**National Institute of  
Standards and Technology**  
U.S. Department of Commerce

**NIST**



**NATIONAL ACADEMY  
OF MEDICINE**

**ECRI** Institute  
The Discipline of Science. The Integrity of Independence.

**ACCE**  
AMERICAN COLLEGE OF CLINICAL ENGINEERING

# My History and Background



VIRTA LABS™



UMASS  
AMHERST



**My opinions are my own and do not necessarily represent or reflect the views of any of my past or current employers**

# Correctness is easy.

---



Photo by Kevin Fu

# Correctness is easy.

---

# Security is hard.



Photo by Kevin Fu

**Wireless medical  
devices:  
great benefits.  
subtle inconvenient risks.**



A Photo by Kevin Fu @ Medtronic museum

1



Kevin Fu, PhD\*  
University of Massachusetts Amherst

Tadayoshi Kohno, PhD\*  
University of Washington

William H. Maisel, MD, MPH\*  
BIDMC and Harvard Medical School

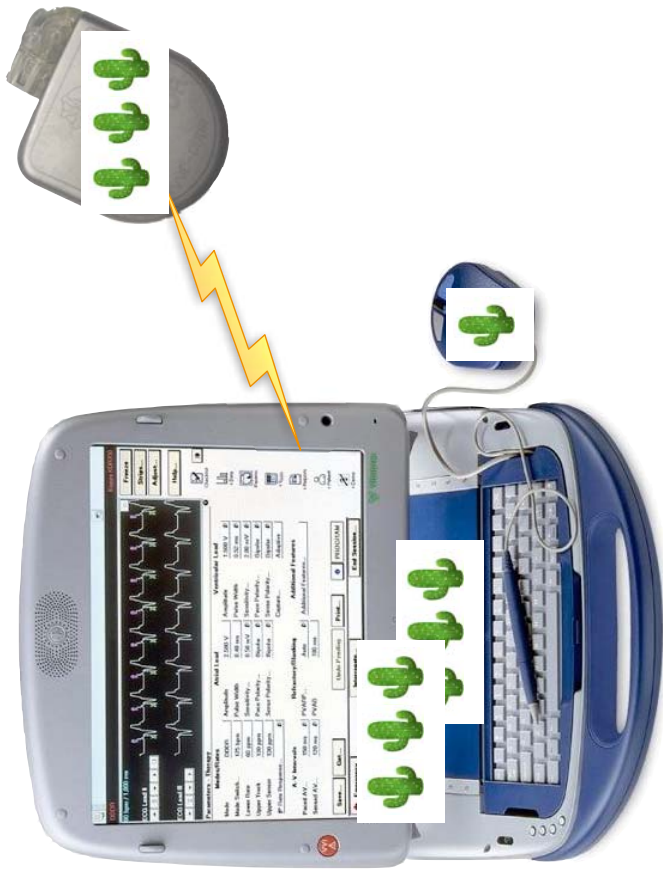
<sup>1</sup>The reader should not confuse the term "device programmer" with a person who programs computers. The former is an external device that communicates with and adjusts the settings on an IMD.






# Implantation of Defibrillator

---

1. Doctor sets patient info
2. Surgically implants
3. Tests defibrillation
4. Ongoing monitoring



Device Programmer

Photos:    ; Video: [or-live.com](http://or-live.com)

# Implanting physician

# compliance physician

# Device state

# Date of birth

Serial no.

... and more

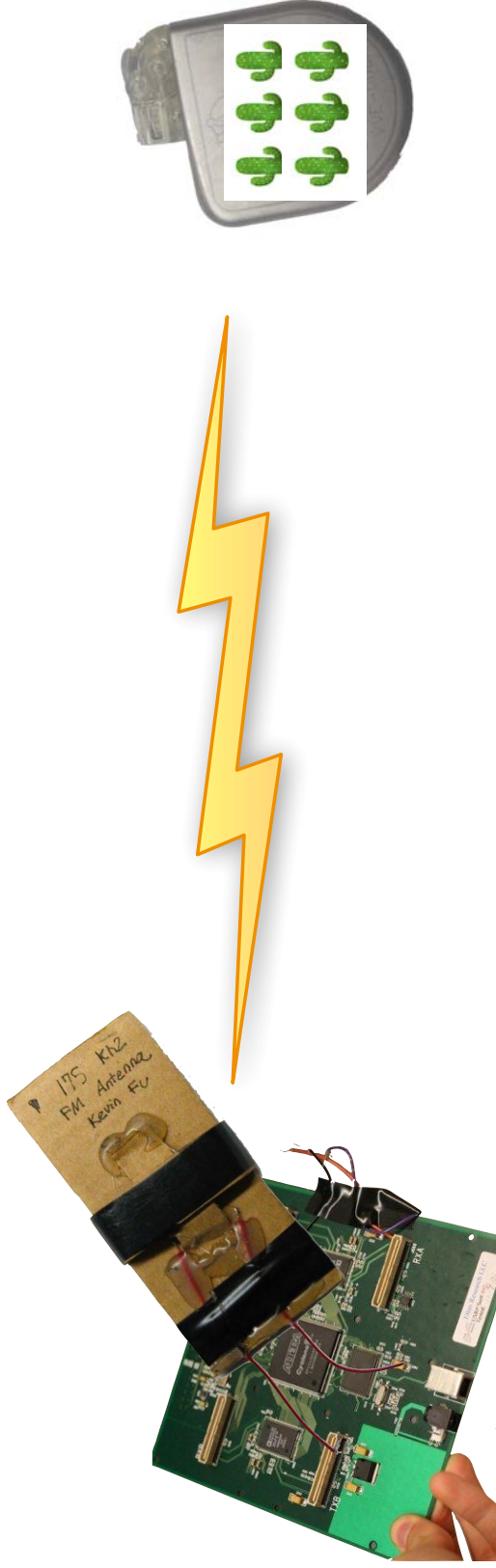
General Hospital

62.....0

⑤

# Wirelessly Induce Fatal Heart Rhythm

- 402-405 MHz MICS band, nominal range several meters
- Command shock sends 35 J in  $\sim 1$  msec to the T-wave
- Designed to induce ventricular fibrillation
- No RF amplification necessary



[Halperin et al., IEEE Symposium on Security & Privacy 2008]

# Modern Healthcare

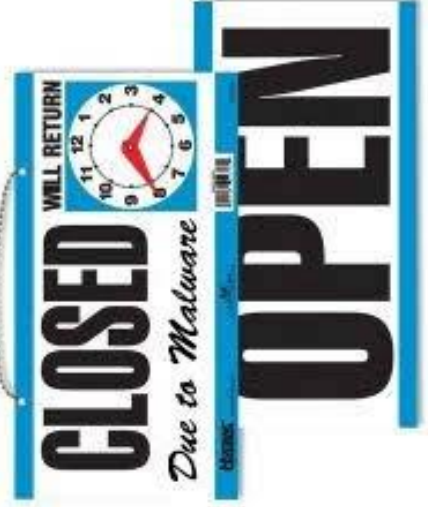
THE ONLY HEALTHCARE BUSINESS NEWS WEEKLY | APRIL 11, 2016 | \$5.50

ITf YOU EV.eR  
WANT TO SEE  
YOUR DATA  
AGAIN

Will hospitals  
pay for security  
to avoid paying up  
as ransomware  
victims? Page 8

Hospitals  
as venture  
capitalists /  
Page 12

Rural  
hospital  
shake-up /  
Page 20



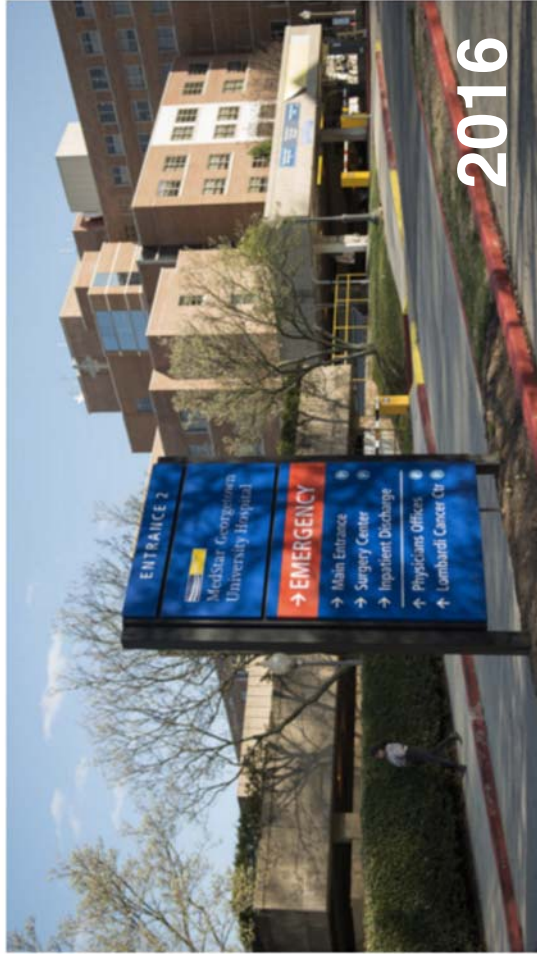
TECH, CULTURE AND CONNECTION

PRIVACY & SECURITY

## Malware Attacks On Hospitals Put Patients At Risk

April 1, 2016 · 4:34 PM ET

NAOMI LACHANCE





## Ooops, your files have been encrypted!

### What Happened to My Computer?

**Y**our important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

### Can I Recover My Files?

**S**ure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)

You can try to decrypt some of your files **for free**. Try now by clicking <Decrypt>. If you want to decrypt all your files, you need to **pay**.

*You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever.*

### How Do I Pay?

**Payment will be raised on**

5/15/2017 16:25:02

Time Left

02:23:58:28

**Your files will be lost on**

5/19/2017 16:25:02

Time Left

05:23:58:28

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)

QR Code

**Send \$300 worth of bitcoin to this address:**



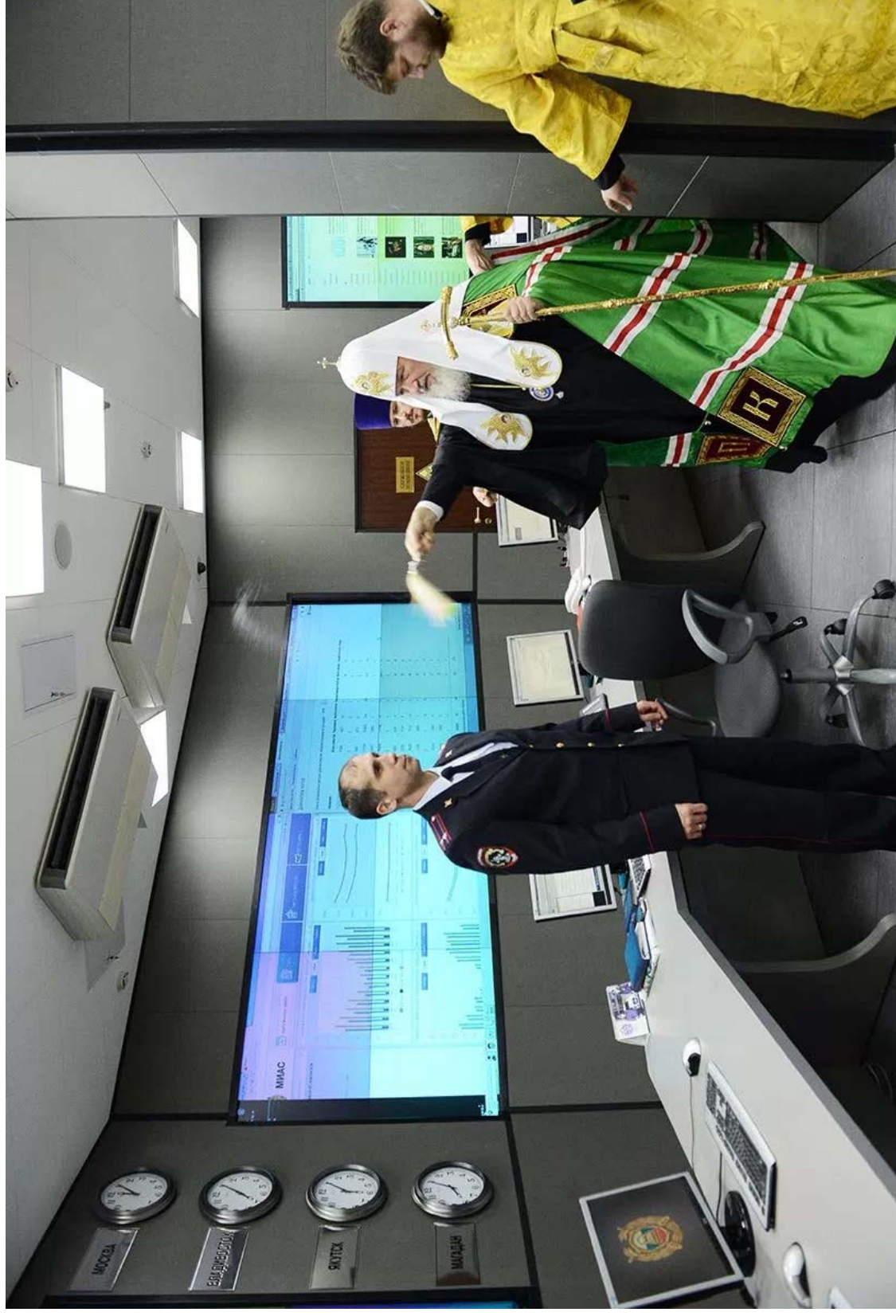
**15zGqZCTcys6eCjDkE3DypCjXl6QWRV6V1**

Copy

Check Payment

Decrypt

## Powerful Russian Orthodox cleric summoned to spritz computers with holy water to fight ransomware



# ← Ways Forward →

Security should  
be **designed** in

not **bolted** on



# AAMI TIR57: Premarket Engineering

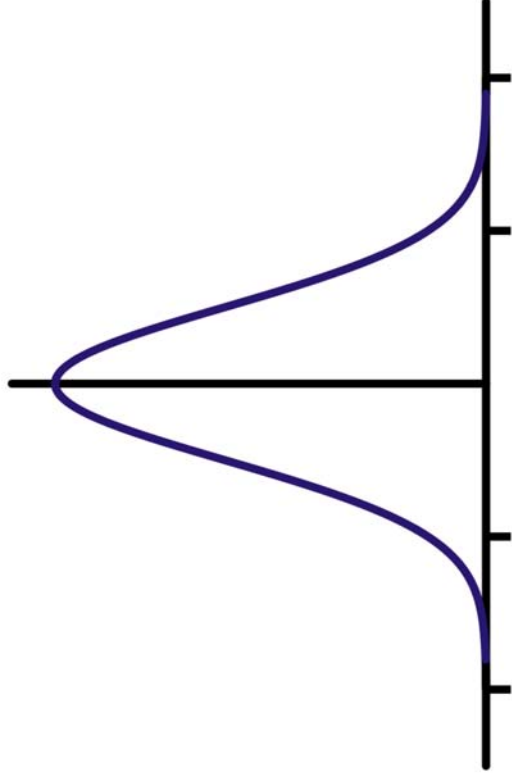
- Principles of medical device security risk management



# Safety :: Security

---

- Safety: Probability distribution normal, mother nature
- Security: Adversary causes the unsafe 1% to be 100%



VS.



# Vulnerability Disclosure & Incidents

---

- Caution: Victim blaming vendors, manufacturers, HDOs
- Meaningful questions to ask:
  - How will medical devices **fail gracefully** when under attack?
  - What mitigating security controls are **designed into** medical devices to continue to function safely **even if hacked**?
  - ~~Is our medical device hackable?~~
  - ~~Has our medical device been hacked?~~
  - ~~Will our medical device be hacked?~~

# Cybersecurity: Patients First

- Biggest risk at the moment:
  - Hackers ~~breaking into~~ medical devices
  - Wide-scale **unavailability** of patient care
  - **Integrity** of medical sensors
- Gaps
  - **Procurement:** HDOs build cybersecurity into contract requirements (e.g., Mayo Clinic vendor book)
  - **Clinical Operations Cybersecurity:**
    - Know your assets cyber risk (e.g., my company Virta Labs)
    - Prioritizing to **clinically relevant** cybersecurity risks. Safety first.
- Challenges
  - Don't interrupt clinical workflow
  - Many security specialists focus on technical controls
  - Many safety specialists focus on risk management



# Reference Slides

---

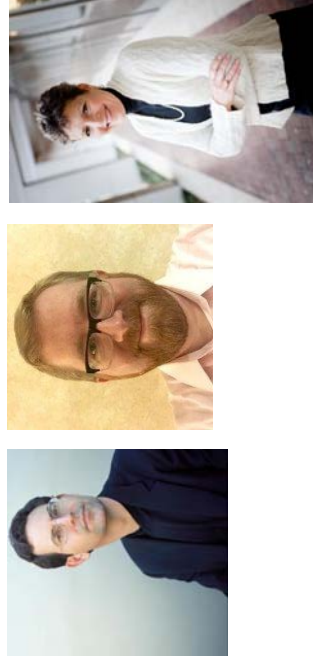
# Related Publications

- "Cybersecurity Concerns and Medical Devices: Lessons From a Pacemaker Advisory" by D. Kramer, K. Fu, JAMA, October 18, 2017 <https://jamanetwork.com/journals/jama/fullarticle/2659246>
- "Cybersecurity and medical devices: A practical guide for cardiac electrophysiologists" by B. Ransford et al. PACE, July 2017 <http://onlinelibrary.wiley.com/doi/10.1111/pace.13102/abstract>
- "Hospitals Need Better Cybersecurity, Not Fear" by Fu et al., Modern Healthcare, September 2016 <http://www.modernhealthcare.com/article/20160914/NEWS/160919950>
- "On the Technical Debt of Medical Device Security" by K. Fu, National Academy of Engineering FOE, September 2015. <https://www.naefrontiers.org/File.aspx?id=50750>
- "Inside Risks: Controlling for Cybersecurity Risks of Medical Device Software" by K. Fu, J. Blum. CACM, October 2013 <http://www.csl.sri.com/users/neumann/cacm231.pdf>
- "Trustworthy Medical Device Software" by K. Fu. In Public Health Effectiveness of the FDA 510(k) Clearance Process: Measuring Postmarket Performance and Other Select Topics: Workshop Report, Washington, DC, July 2011. IOM (Institute of Medicine) <https://spqr.eecs.umich.edu/papers/fu-trustworthy-medical-device-software-IOM11.pdf>
- "Reducing the Risks of Implantable Medical Devices: A prescription to improve security and privacy of pervasive health care" by K. Fu, CACM 52(6), June 2009. <http://www.csl.sri.com/users/neumann/insiderisks08.html#218>
- "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses" by D. Halperin et al. In IEEE Symposium on Security and Privacy, May 2008. <https://www.secure-medicine.org/public/publications/icd-study.pdf>

## Cybersecurity and medical devices: A Practical guide for cardiac electrophysiologists

Benjamin Ransford PhD, Daniel B. Kramer MD, MPH, Denis Foo Kune PhD,  
Julio Auto de Medeiros, Chen Yan, Wenyuan Xu PhD, Thomas Crawford MD,  
Kevin Fu PhD 

Accepted manuscript online: 17 May 2017 Full publication history



## Modern Healthcare

# Commentary: Hospitals need better cybersecurity, not more fear

By Kevin Fu, Dr. John Halamka, Jack Kufahl and Mary Logan | September 14, 2016

We've seen unprecedented attention to medical-device security after an **unorthodox report** was recently released by short-selling investment research firm Muddy Waters Capital and MedSec, which alleged security vulnerabilities in **St. Jude Medical's** pacemakers. An **independent research team** subsequently raised doubts about some of the clinical claims made by the report. St. Jude Medical, meanwhile, has filed a lawsuit disputing the allegations in the same report.

VIRTA LABS™



Making Sense of  
Muddy Waters & MedSec

Industry White Paper  
September 1, 2016 (Updated April 18, 2017)  
info@virtalabs.com

Public Release  
Copyright 2017 Virta Laboratories, Inc.  
All rights reserved.

## Healthcare IT News

TOPICS  SIGN UP

MAIN MENU 

# Ransomware: How we can climb out of this mess

## Privacy & Security

Healthcare security experts argue that hospitals must ensure high availability of medical devices and IT systems with practices that resemble preventing and treating disease. Because ransomware is a symptom rather than the problem.

By **Kevin Fu** and **Harold Thimbleby** | June 05, 2017 | 07:04 AM

